48th Closed Session of the Global Privacy Assembly

November 2026

Resolution on Privacy-Enhancing Technologies as Instruments of Privacy by Design and Data Protection Accountability

This Resolution is submitted by CNDP, the Data Protection Authority of Morocco

SPONSORS:

- Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel (CNDP) - The Data Protection Authority of Morocco

CO-SPONSORS:

- Agencia de Acceso a la Información Pública (AAIP), Argentina
- Commission for Personal Data Protection (CPDP), Bulgaria
- Office of the Privacy Commissioner (OPC), Canada
- Office of the Information and Privacy Commissioner, Ontario, Canada
- Commission Nationale de l'Informatique et des Libertés (CNIL), France
- Privacy Protection Authority (PPA), Israel
- Federal Commissioner for Data Protection and Freedom of Information (BfDI), Germany
- Office of Data Protection Authority (ODPA), Guernsey
- Autoridade Nacional de Proteção de Dados (ANPD), Brazil
- Information Commission's Office (ICO), United Kingdom

Restricted Use - À usage restreint

The 48th Global Privacy Assembly 2026:

Acknowledging that Privacy-Enhancing Technologies (PETs) are understood as a collection of methods, processes and digital tools designed to support the protection of personal data, and thus the privacy of the data subjects;

Being aware of the potential for PETs to bring important economic, societal, and public interest benefits by enabling privacy-preserving processing within organisations and data collaboration across sectors, including healthcare, finance, research, and public administration, and across jurisdictions by supporting data free flow with trust (DFFT) where applicable, while respecting individuals' fundamental rights and freedoms;

Emphasising the shift toward Privacy by Design architectures, and the growing importance of accountability-based frameworks in which data controllers proactively implement and demonstrate compliance with data protection principles rather than delegate such compliance to individuals;

Recognising that PETs encompass a diverse and evolving taxonomy of technologies, including, but not limited to, data obfuscation tools (synthetic data, differential privacy, zero-knowledge proofs), encrypted data processing tools (homomorphic encryption, secure multi-party computation, private set intersection, trusted execution environments), federated learning and distributed analytics, and documentation and transparency tools;

Acknowledging that PETs, when implemented properly, can serve as concrete technical instruments that contribute to support compliance with legal obligations arising from data protection frameworks, including the principles of data minimization, purpose limitation and data protection by design and by default as recognised in applicable national, regional, and international data protection laws;

Being mindful that the maturity, implementation cost and complexity of PETs vary significantly across technologies;

Recognising the particular relevance of PETs for the development and deployment of artificial intelligence (AI) systems, where they may enable privacy-preserving model training and collaborative AI development;

Recalling existing GPA resolutions that emphasise accountability, transparency, and the right of individuals to exercise control over their personal data, and which call on data protection authorities to promote the adoption of technical safeguards as part of responsible data governance;

Taking note of concrete implementations of PETs in several countries, including in the public sector, demonstrating the operational feasibility of privacy-preserving data use;

Recognising that PETs are not a substitute for legal compliance or sound governance, and that they must be accompanied by appropriate procedures, testing, auditing, and complementary organisational measures in order to be effective;

Recognising also that coordinated work is required across legal, policy and technical frameworks, including aligning protection requirements with relevant technical standards, frameworks (e.g., ISO/IEC, NIST, IEEE and IETF standards) and certification mechanisms; and acknowledging that the continued development of internationally recognised standards for certain categories of PETs would support cross-border interoperability and greater regulatory coherence;

Recognising that meaningful implementation of PETs requires sustained investment in capacity building, including, *inter alia*, technical training, awareness programmes, and the development of human expertise, among data controllers, data protection authorities, and policymakers, as well as in the technology sector at large, and that the open-source ecosystem plays a strategic role in democratising access to privacy-preserving tools;

Emphasising the need for reinforced international cooperation to harmonise technical standards and regulatory approaches to PETs, including through the development of common certification mechanisms, auditing frameworks, information on enforcement actions and repositories such as the OECD Global Repository for PETs.

The 48th Global Privacy Assembly therefore resolves to:

1. Promote a common understanding among data protection authorities of the nature, taxonomy, categorisation, capabilities, and limitations of Privacy-Enhancing Technologies, as well as the conditions under which their deployment constitutes an effective contribution to privacy by design, data minimization, and accountability obligations;

2. Urge organisations that process personal data to consider the deployment of appropriate PETs as part of their privacy by design and by default obligations, proportionate to the risk, context, and scale of their data processing activities, and to ensure that such deployment is accompanied by adequate governance, training, documentation, testing, monitoring and audit procedures;

3. Acknowledge that minors are particularly vulnerable in digital environments, and that PETs could serve as essential safeguards for reducing privacy risks and strengthening their protection;

4. Encourage data protection authorities to continue to develop and publish guidance on the use of PETs that is accessible to organisations lacking specialised technical expertise and small-scale data controllers and processors, including practical guidance on selecting appropriate PETs for given processing contexts and risks they intend to address, their interaction with applicable legal standards, and the conditions under which their use may serve as evidence of compliance with data protection obligations;

5. Call on data protection authorities, in cooperation with standardisation bodies, research institutions, and industry, to support the development of harmonised technical standards and certification mechanisms for PETs, including common assessment criteria to guide PETs providers and evaluate their solutions;

6. Encourage the establishment and sharing of experiences regarding regulatory sandboxes and innovation spaces that allow organisations to test PETs in real-world conditions under the guidance of data protection authorities, thereby accelerating their maturation and responsible adoption;

7. Call for reinforced collaboration between data protection authorities and AI regulators to ensure that PETs are systematically considered within data protection impact assessments, algorithmic accountability frameworks, and the governance of AI systems that process personal data at scale, recognising the potential role of PETs in enabling privacy-preserving AI development and deployment;

8. Share knowledge and best practices through the GPA Working Groups regarding the practical implementation of PETs within members' respective legal frameworks, including case studies of public sector deployments, regulatory approaches, audit methodologies and to develop resources for data protection authorities to support the promotion of PETs adoption by controllers and processors in their jurisdictions;

9. Promote the development of open-source PETs libraries and research infrastructure as strategic public assets that support data protection and privacy, transparency, auditability, and technological sovereignty, and encourage data protection authorities to engage with open-source communities and academic institutions as key actors in the PET ecosystem;

10. Support international cooperation in developing academic and professional education initiatives on PETs and uses to promote compliance and data protection across domains and applications;

11. Promote the implementation of mechanisms for international knowledge exchange, including virtual meetings, physical workshops, short-term expert exchange and internship programs, involving participants from the public sector, academia and industry.

The United States Federal Trade Commission abstains from the adoption of this resolution.